UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (JMF)

MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S MOTIONS *IN LIMINE*

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

David W. Denton, Jr.
Michael D. Lockard
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

RULES

The Government respectfully submits this memorandum in opposition to the defendant's motions *in limine* (D.E. 776, the "Motion") seeking to preclude the Government from offering various evidence and argument relating to the MCC Leak Charges[1] (Mot. at 2-10); to preclude the Government from offering certain digital evidence (Internet Relay Chats) recovered from the defendant's home server, which the defendant previously stipulated was admissible (*id*. at 11-12); to preclude the Government from offering evidence produced in discovery in response to particularized defense requests (*id*. at 13-14); and to permit the defendant to offer "public news organizations . . ., the WikiLeaks website, blogs and other articles" as evidence that the classified information the defendant disclosed and attempted to disclose in connection with the MCC Leak Charges was not "closely held" (*id*. at 15). The Motion also asks for an order that the trial be audio- and video-recorded "for later publication" and to reject certain witness protection measures and partial courtroom closure procedures. (*Id*. at 14).

ARGUMENT

I. Evidence from the MCC Notebooks, and Argument Relating to that Evidence, Are Admissible and Proper

A. Relevant Background

As described in the Government's Motions *In Limine*, following his arrest Schulte violated the Court's discovery Protective Order and disclosed and attempted to disclose classified information while detained at the MCC. Schulte (i) emailed a reporter a copy of a search warrant affidavit, thereby violating the Protective Order, and a document containing classified national defense information about Hickok, a classified CIA computer network (GX 812); (ii) drafted and

[1] This memorandum uses the same defined terms as the Government's Motions *In Limine* (D.E. 780).

prepared for dissemination the Schulte Article (*infra* at 13); and (iii) attempted to transmit tweets about a classified CIA cyber tool (GX 809) and an article titled "Malware of the Mind" containing classified information about CIA tradecraft (the Malware Article) (GX 801). Schulte accomplished this by using contraband cellphones smuggled into the MCC, from which he established various pseudonymous email and social media accounts to communicate with the outside world.

Notes from Schulte's MCC Notebooks reflect his plans to wage his "information war," which consisted of multiple anticipated prongs of attack. One prong was to publish manufactured statements of support from imaginary colleagues and FBI agents, protesting Schulte's innocence and claiming that the evidence against him was fabricated. A second prong was to publish his first-person screeds about his case, including complaints about his interview by law enforcement, the search of his apartment, his bail proceedings, and searches of his electronic accounts. These articles were peppered with confidential and classified information. A third prong was to draft social media postings disclosing classified information about tools and projects that Schulte worked on while at the CIA. Schulte's goals included attempting to drum up public support for his case by portraying himself as an innocent victim of a corrupt criminal justice system and causing harm to the United States and its intelligence and diplomatic interests.

On a page from the MCC Notebooks bearing the date "Wednesday 8/8," Schulte wrote, among other things:

> If govt doesnt pay me $50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery that is the USG. I will look to breakup diplomatic relationships, close embassies, and U.S. occupation across the world & finally reverse U.S. jingoism. If this is the way the U.S. govt treats one of their own how do you think they treat allies?

(GX 809 at 2). On a page dated six days later, "Tuesday 8/14," Schulte wrote, among other things:

> Got to use last night.[2] The way is clear. I will setup a wordpress of joshschulte.wordpress.com and presumption of innocence.wordpress.com. From here, I will stage my information war:
>
> Facebook I will rename, simply, "Who is John Galt?"[3] or "Who is Josh Schulte?"
>
> From FB, I will post links to the articles and blogs as I write them.
>
> The presumption of innocence blog will only contain my 10 articles 1-10, ending on the presumption of innocence. I will post each of them on the FB & delete the previous articles.
>
> From my blog, I will write about my time, etc.

(*Id*. at 3). Later pages from the MCC Notebooks reflect Schulte's attempts to get copies of his 10 articles, which he started writing before his bail was revoked, from family members. (*Id*. at 4).

On a page from the MCC Notebooks dated one week later, "Tuesday 21st," Schulte wrote, in part: "They got IMEI of my phone [U/I] subpoena of phone #," reflecting his understanding of how his telephonic and online activities could be investigated. Additional notes reflect his efforts to destroy evidence and enhance the security of the contraband cellphones and his email and social media accounts based on that concern, with apparently completed tasks checked off and remaining tasks circled:

> √ 1.) Delete all Google Docs from johnsmith
>
> √ 2.) Delete all emails from johnsmith
>
> (3.) Delete suspicious emails from my gmail
>
> a.) New logons from phones
>
> b.) Paypal

---

[2] Schulte appears to be referencing one of the contraband cellphones.

[3] John Galt is a fictional character from *Atlas Shrugged* by Ayn Rand.

c.) Wordpress

√ d.) PW changes

√ 4.) Create new protonmail: presumedguilty@protonmail.com

√ 5.) Migrate wordpress to protonmail

6.) Clean off apps

7.) Reset factory phone

(GX 809 at 5). Additional notes on the same page reflect Schulte's concerns about whether Google retained copies of deleted emails and how to disguise or change the IMEI number on the contraband cellphones, as well as his plans to use "all different phone numbers" for electronic messaging apps to frustrate investigative efforts. (*Id.*).

On a page bearing the date "Thursday August 23rd," Schulte documented his destruction of evidence: "Yesterday I started clensing [sic] the phone . . ." (GX 809 at 7). He also described his frustrations with family members having posted the wrong versions of his articles, and having posted only some of them. "They decided FOR ME not to publish the articles – well, rather, not to give me my own fucking articles. Isn't that incredible? They fucked up to begin with & published the wrong (old!) versions THEN they didn't publish the two most important parts (8 & 9) and now they are withholding ALL of them." (*Id.*). On the same page, Schulte wrote: "Yesterday I started emailing [a reporter] from the Washington Post." (*Id.*). On a following page, Schulte wrote about getting copies of his articles from the reporter by pretending to be Schulte's cousin so that he could edit and publish "my 9 articles." He also wrote about rewriting "article #10: Malware of the Mind!" (*Id.* at 8).

Schulte also drafted social media postings, written as other individuals, discussing Schulte and classified information. One description of Schulte described him as "the cyber representative [redacted/classified] on behalf of USG." (GX 809 at 8). In another post intended for the Twitter

account "FreeJasonBourne,"[4] created by Schulte, Schulte wrote in the voice of a purported former colleague and claimed Schulte was a "scapegoat" because Schulte reported security issues at the CIA (a false claim). The post included the classified true name of a covert CIA developer. (*Id*. at 9). To establish the imaginary colleague's credentials, the post included classified information about a CIA cyber tool called Bartender: "Just to authenticate me first. The @CIA was involved in [redacted/classified] the code for initially-planned cyber operation is in Vault 7. Additionally, [Tool described in vendor report] [classified] is in fact Bartender. A CIA toolset for [operators] [classified] to [redacted/classified] configure for deployment." (GX 809 at 10).

On another page, Schulte continued his draft social media posts by manufactured colleagues, including the disclosure of classified information, and his planned hashtags—including "#FuckYourTopSecret"—and "or dump the secrets here." Schulte wrote:

> Let me first establish credibility ~~authenticate~~ myself. The USG was involved in the [redacted/classified.] Source code for the planned [redacted/classified] cyber espionage component is in the Vault 7 release.
>
> The @CIA conducted numerous operations against [redacted/classified] and [redacted/classified.] Source code is available in the Vault 7 release.
>
> [@vendor/classified] discussed [tool/classified] in 2016, which is really the CIA's Bartender tool suite. [Redacted/classified] Bartender was written [redacted/classified] to deploy against various targets. The source code is available in the Vault 7 release.
>
> Vault 7 contains numerous zero-days and malware that could easily be ~~deployed~~ repurposed and released onto the world in a devastating fashion that would make Notpetiy[5] look like child's play. [redacted/classified].

---

[4] Jason Bourne is a fictional CIA operative from the *Jason Bourne* series of movies.

[5] This appears to be a reference to NotPetya, a cyber attack malware that caused significant damage in approximately 2017 and 2018. *See, e.g.*, Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED MAGAZINE (Aug. 22, 2018),

(GX 809 at 11).

On another page, Schulte drafted another message encouraging others to disclose classified information (and reflecting his own desire and intent to disclose classified information): "To the United States Intelligence Community – why would you keep ~~America's~~ the govt's secrets when ~~your own country~~ the govt wrongly prosecutes your own?" (GX 809 at 12). Schulte then drafted another post disclosing the classified true name of a covert CIA developer. (*Id.*). On another page, Schulte expanded on his call, written in the third person voice, for others to disclose additional classified information:

> Your service, intense security investigations, and pristine criminal history cant even get you bail. As Josh Schulte has said, you are denied a presumption of innocence. Ironic, you do your country's dirty work but when your country accuses you of a crime you are arrested & presumed guilty. Until your ~~country~~ govt protects you and honors your service, send all your govt's secrets here: WikiLeaks.
>
> This is a HUGE wake-up call to U.S. intelligence officers. The Constitution you fight to defend will be denied to you if, God forbid, you are ever accused of a crime. If your own govt has no allegiance in you, why do you have any allegiance toward your govt?
>
> (our associates provided info to the NYT)

(GX 809 at 13) (emphasis supplied).

Other pages of the MCC Notebooks reflect Schulte's plan to release the tweets he drafted, which included classified information, during the month of September. On a page dated "9/12," Schulte wrote: "Finalize copy by Friday," "Edit during weekend Sat; Sun; finalize," "Monday 17th - Tues

---

available at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

18th: DL Disc, UL WL;" "*19, 20, 21: Schedule tweets 27th*; send tech reports MCC letter, Russia piece; *Rest 22-25*." (GX 809 at 15) (emphasis supplied).

B. Discussion

As set forth in the Government's renewed motion *in limine* with respect to evidence of the defendant's prison conduct, this evidence—including the evidence described above—is direct evidence of Schulte's commission of the MCC Leak Charges and is relevant evidence under Rule 404(b) with respect to Schulte's identity, motive, intent, preparation, and planning with respect to the WikiLeaks Charges, and the Court admitted this evidence at the prior trial. (D.E. 195 at 27-48; D.E. 780 at 16-17). In his motions *in limine*, however, Schulte argues that the Government should be precluded from arguing to the jury entirely permissible inferences from his own statements. He argues that the Government should be precluded from (i) arguing that Schulte's "information war" means anything other than Schulte's current, self-serving description, that is, the publication of "unclassified Redress of Grievances" articles (Mot. at 8-9); (ii) introducing Schulte's statement that "If govt doesnt pay me $50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case" he would "look to breakup diplomatic relationships, close embassies, [and] end U.S. occupation across the world . . . ." because, Schulte claims, he was referring only to legal actions (*id*. at 9); (iii) arguing that Schulte intended to send classified information to WikiLeaks from the MCC (*id*.);[6] (iv) arguing that Schulte "promised to give

[6] The Government does not intend to argue that WikiLeaks was necessarily the intended recipient of the classified information Schulte attempted to transmit from the MCC, although Schulte's notes appear to suggest that he intended to upload discovery productions to WikiLeaks (GX 809 at 15 ("DL Disc, UL WL"). Schulte did, however, intend to exhort other holders of classified information to send secrets to WikiLeaks. (*Id.* at 11 ("#TopSecret[,] #FuckYourTopSecret → or dump the secrets here!"), 13 ("send all your govt's secrets here: WikiLeaks")).

classified information to reporters" (*id*. at 10); (v) arguing that Schulte created email and social media accounts at the MCC "specifically to post 'classified articles'" (*id*.); (vi) arguing that Schulte "wrote a detailed battle plan to destroy evidence and leak classified information" (*id*.); or (vii) arguing that Schulte's plan to disseminate classified information from the MCC was thwarted by the FBI (*id*.).

Schulte's arguments rely on his own self-serving explanations for his own words and writings in the MCC Notebooks, draft tweets, draft articles, and email communications with reporters. Schulte is free to argue to the jury that his intentions and actions were innocent, but the Government also is free to argue the permissible inferences that Schulte intended to disclose classified information. Even on the page of the MCC Notebooks where Schulte refers to his "information war," Schulte makes clear that the war is not limited to the publication of what Schulte refers to as Redress of Grievances. (GX 809 at 3). He describes posting "links to articles and blogs as I write them," anticipating more than just the Redress of Grievances articles. Only six days before describing his "information war," Schulte described his intention to engage in very war-like retaliatory measures: visiting other countries in order to "breakup diplomatic relationships, close embassies," and "end U.S. occupation" (*i.e.*, military operations) "across the world." (*Id*. at 2). It defies common sense that Schulte expected to breakup diplomatic relationships and close embassies through legal action. It is entirely proper for the Government to argue that the jury may infer Schulte's intent to disclose classified information for the purpose of damaging U.S. foreign relations.

On a page dated only a week after his reference to his information war (*id*. at 5), Schulte made a to-do list to destroy evidence, deleting emails and documents, establishing new encrypted accounts, and researching the masking of the IMEI on his Contraband Cellphones. The very next

page lists Schulte's unattributed Facebook, WhatsApp, Signal, Protonmail, and Gmail accounts and passwords. (*Id*. at 6). Two days later, on a page dated August 23, Schulte wrote about contacting a reporter. (*Id*. at 7). In those communications, where Schulte posed as his own associate, Schulte promised the reporter "snippets of text of the two articles 8 and 9 that weren't release publicly to verify my access to Josh and Shane [Presnall]." (GX 1303-3). On August 23, Schulte sent two "snippets" (GX 1303-5), as well as later emails that included full names of CIA personnel (GX 1303-35). Schulte also asked the reporter's help in publicizing a "press release" that Schulte planned to post to the John Galt Facebook page on his birthday. (GX 1303-35). On September 1, 2018, Schulte opened the "freejasonbourne" Twitter account (GX 1304-1, -2, -3), the platform from which he intended to tweet his draft messages posing as other people and disclosing classified information. (GX 809 at 9-13). And in an email exchange with the reporter between September 22 and 24, 2018, Schulte sent documents that included classified information about CIA networks and the sizes and interactions of the cyber groups that used them. (GX 812).

From these concrete facts, the jury is entitled to infer that Schulte's reference to an "information war" included, among other things, the publication of classified information in an effort to sway public opinion about his prosecution and to harm U.S. national interests, including by releasing information to reporters, posting articles on social media and tweeting messages on Twitter; and that his MCC Notebooks contain detailed planning in connection with this effort. The jury is also entitled to infer that Schulte's reference to demanding $50 billion was in connection with his desire to harm U.S. foreign relations through the disclosure of classified information. These inferences are not speculative, but clear and reasonable inferences from Schulte's own words and pattern of conduct. His plan was, indeed, foiled by the FBI when a warrant to search Schulte's cell was issued on or about October 2, 2018. These clear inferences about the defendant's

state of mind support the element of the MCC Leak Charges that the defendant willfully communicated national defense information to a person not entitled to receive it, and that the defendant took a substantial step in an effort to bring about the willful communication of national defense information to a person not entitled to receive it. This evidence is also proper under Rule 404(b) to show the defendant's state of mind in committing the WikiLeaks Charges.

Schulte's motion to limit reasonable inferences and argument, soundly grounded in the evidence, should be denied.

II. The Internet Relay Chats Are Admissible

A. Relevant Background

Among the evidence recovered from the defendant's New York City apartment during the court-authorized May 16, 2017 search was a home server that stored Internet Relay Chats ("IRCs"). (Tr. 2241-42). The defendant was asked about the IRCs, and he acknowledged that he and a group of friends communicated by IRC and that the defendant's name in the chats was "Josh." (Tr. 2242). Several IRCs were received in evidence pursuant to stipulation at the prior trial. (Tr. 638-41, 2242-48; GX 1405-1 – 1405-12; GX 3003). In one IRC, the defendant responded to a friend sharing a link to an article about effective liars with the comments: "I'm a rather natural manipulator myself ;-);" "I would always get my way when I was young[,] whatever was necessary;" "I could lie to anyone and get away with it[.]" (GX 1405-2). In another IRC the defendant admitted to copying files from his classified CIA computer and bringing them home to work on them, which was not classified "according to me." (GX 1405-5). In another IRC discussing the Manning leak, the defendant said—referring to the classified systems he worked on—"the security is simply dependent on the people hired to protect it[,] the system itself is pretty invulnerable[,] it's the people who fuck it up[.]" (GX 1405-8).

B. Discussion

Schulte asks to preclude the IRCs because, he asserts, the IRCs were logged by user-written programs and could be manipulated by individuals with access to the server. (Mot. at 11-12). Schulte's motion should be denied for two reasons. First, he already stipulated to the admissibility of the IRCs. *See* Government's Motions *in Limine* (D.E. 780) at 18-20. Second, the challenges Schulte raises to the authenticity of the IRCs go, at most, to their weight and not to their admissibility. The authenticity of the IRCs is established by (1) evidence that they were obtained from the defendant's home server; (2) the defendant acknowledged that they were IRCs; and (3) the defendant acknowledged that his username in the chats was "Josh." In his motion, the defendant does not even challenge that the chats are what they purport to be, that is, records of electronic communications between the defendant and his friends or associates. He argues only that they are open to potential manipulation. The Second Circuit has held that "[A]llegations of tampering went to the weight of the evidence, not its admissibility." *United States v. Sovie*, 122 F.3d 122, 127 (2d Cir. 1997).

Schulte also argues that the IRCs are not responsive to the warrant to search his apartment. (Mot. at 12). This argument, too, is precluded by his prior stipulation to the admissibility of the IRCs. Moreover, the defendant has never previously moved to suppress the IRCs, and his deadline for doing so has long passed. (*See* D.E. 650 (setting deadline for new pretrial motions)). In any event, the defendant's late contention that the IRCs exceed the scope of the warrant is also incorrect. The warrant authorized the seizure of, among other things, (1) evidence concerning the ownership or occupancy of the subject premises (*i.e.*, the defendant's apartment); (2) records pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials; and (3) evidence indicating computer users' state of mind as it relates to the subject offenses of

espionage and unauthorized computer access. The IRCs fall into all three categories: the fact that the defendant is one of the participants in the IRCs stored on the server is evidence that he owned and controlled the subject premises; the IRCs reflect communications about the unauthorized removal and retention of classified materials by the defendant; and the IRCs reflect the defendant's state of mind with respect to the offenses of espionage and unauthorized computer access.

The defendant's motion to preclude the IRCs should be denied.

III. GX 1207-27 and 1207-30 Are Admissible

A. Relevant Background

The evidence at trial will include a large volume of forensic computer data obtained from CIA computer systems, including from the workstation used by Schulte during his employment there and from relevant components of the CIA network housing the DEVLAN system; and from Schulte's home computer and electronic devices seized from his New York City apartment. Among these are GX 1207-27 and GX 1207-30, which were introduced at the prior trial. Both exhibits are from the Confluence backup folder on Altabackup, the location on the NetApp server where backup files were stored. (Tr. 940, 953-54). The Confluence backup folder stored the daily Confluence backups, which were stored as a SQL database file and a corresponding .zip file. (Tr. 955-56). The date accessed information for these backup files shows that the backup created on March 3, 2016, was last accessed on April 20, 2016, at 5:42 and 5:43 p.m., which is the time during which Schulte had reverted the Confluence virtual machine to its April 16, 2016 state—a state in which Schulte's administrator privileges had not yet been revoked.

B. Discussion

Schulte argues that GX 1207-27 and 1207-30 should be precluded because "the government hid relevant, critical forensic images from the defense, and forced the defense to reveal defense strategy and privileged information to obtain access to specific data." (Mot. at 13-14). The

Government's disclosures, however, were in compliance with the Court's orders pursuant to CIPA, and the defendant's complaint about GX 1207-27 and 1207-30 is based on their incriminating nature rather than on any disadvantage he purportedly suffered from the supposed disclosure of defense strategy.

It is undisputed that the NetApp server contains large volumes of highly classified data that is irrelevant to the charges in this case and unhelpful to the defense. (D.E. 124 at 11-12). For this reason, the Court has repeatedly rejected Schulte's requests for wholesale access to the entire server. (*See* D.E. 124, 514). The Court recognized that "the Government has put a great deal of planning and effort in collecting, reviewing, and producing what might be an unprecedented volume of classified discovery to Schulte" (D.E. 124 at 11; *see also* D.E. 514 at 4 ("the parties have coordinated the disclosure of a substantial volume of classified data")); as well as the fact that "the Government and Schulte have been cooperating to resolve discovery disputes" with respect to data from the CIA computer systems. (D.E. 124 at 12-13). While the Court denied the defendant's request for wholesale disclosure of the classified computer systems, it left "open the possibility of ordering production of forensic data . . . if Schulte submits a more tailored request and provides good reason for further forensic discovery in a motion to compel." (*Id*. at 12; *see also* D.E. 514 at 5-6 ("the Court again leaves open the possibility of ordering additional production of forensic data if Schulte submits, and can justify, a more tailored request")).

The fact that the Government satisfied "more tailored request[s]" for classified discovery (D.E. 514 at 3 (quoting D.E. 124 at 12)) from the NetApp server, and that the underlying information was incriminating, is no basis for preclusion.

Moreover, Schulte does not articulate how his expert's request for the data reflected in GX 1207-27 and -30 reveals any defense strategy. His argument is not that the Government gained an

unfair advantage in rebutting his expert's analysis; it is simply that the evidence is incriminating. Nor does Schulte cite any authority for the proposition that he is entitled to shield his expert witness's analysis from disclosure in any event. To the contrary, any analysis by his expert would be required to be disclosed under Rules 16(b)(1)(C) and 26.2, just as the Government made voluminous expert discovery available to the defendant under Rule 16(a)(1)(G) and 18 U.S.C. § 3500. The motion to preclude should be denied.

IV. Schulte Should Be Precluded from Offering Unspecified Websites, Blogs, and Articles Regarding WikiLeaks' Unlawful Disclosures

A. Relevant Background

The defendant moves to admit "public websites, including new[s] organizations (New York Times, Washington Post), the WikiLeaks website, blogs and other articles, to illustrate that the MCC Charges are predicated on materials not 'closely held' by the government." (Mot. at 15). Beyond this general description, the Motion does not identify what particular articles, blogs, or websites the defendant intends to offer. Schulte relies on his memorandum filed pursuant to CIPA § 6 in support of his argument that these articles are relevant to whether national defense information is "closely held."

B. Discussion

The defendant articulates one narrow ground of relevance for his request to admit an unknown quantity of unidentified news articles, blogs, and websites: the question of whether information the defendant disclosed and attempted to disclose from the MCC was "closely held." The fact of the Leaks is not disputed at trial and, indeed, is a central feature of the Government's case. The Government is mindful of the Court's recent order concluding that "evidence tending to show that the information in the 'documents, writings, and notes' Defendant is charged with communicating and attempting to communicate in Counts 3 and 4 of the Third Superseding

Indictment was publicly available at the time of the charged conduct is not categorically irrelevant or inadmissible" (D.E. 800 at 1), but additional, unspecified news coverage of the Leaks, or descriptions and commentary by unidentified bloggers, is cumulative of the Leaks themselves and lacks any additional probative value.

Moreover, there are only narrow grounds on which press articles can be competent evidence. "Newspaper articles are ordinarily inadmissible hearsay if sought to be entered into evidence for the truth of the matter asserted therein. However, articles offered not for the truth of the statements made therein, but rather to show that a party had notice about a specific set of facts are sometimes admissible as non-hearsay evidence." *United States v. Buck*, No. 13 Cr. 282 (JSR), 2017 WL 5201447, at *2 (S.D.N.Y. Oct. 30, 2017) (internal citations omitted). This is *not* the basis for relevance that Schulte advances, but even to fit within that narrow exception, the proponent of such evidence must demonstrate the "relevance of the specific articles and the likelihood the defendant would have read them," *i.e.*, "the connection, if any, between the articles and the defendant." *Id.* at *3. Thus, in order to be relevant to any argument that the defendant did not act willfully in disclosing and attempting to disclose classified information as charged in Counts Three and Four, the defendant must first proffer an evidentiary foundation to believe that particular articles affected his state of mind. The fact that articles exist and could have been read by others alone is not sufficient. Here, the defendant has not even identified the particular articles and websites he seeks to offer, much less proffered the necessary foundation for their admissibility. Accordingly, the Court should not permit the introduction of any articles until there is a suitable record in the evidence—and not merely in the defendant's argument—to believe that there is a non-hearsay purpose for which such evidence will be used.

V. The Court's Standing Orders Prohibit Audio- and Video-Recording of the Trial

The defendant's motion *in limine* includes requests that the Court record the trial proceedings for later public dissemination. (Mot. at 14). The standing orders of the Southern District of New York prohibit the recording of trials and the defendant offers no basis for challenging these standing orders. *See, e.g.*, Local Cr. R. 1.1(b) (incorporating specified Local Civil Rules) & Local Civ. R. 1.8 (prohibiting audio or video recording of proceedings absent an administrative order of the Southern District of New York); Standing Order, M10-468 (REVISED), Dkt. No. 14 Misc. 0047 (S.D.N.Y. Feb. 27, 2014), para. (k).[7]

CONCLUSION

For the foregoing reasons, the Government respectfully submits that the Court should deny the defendant's motions *in limine* and for other relief.

Dated: New York, New York
May 13, 2022

Respectfully Submitted,

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

By: /s/
David W. Denton, Jr.
Michael D. Lockard
Assistant United States Attorneys
(212) 637-2744 / -2193

cc: Joshua Adam Schulte (by mail)
Standby counsel (by ECF)

[7] The defendant also opposes the Government's request for witness security measures (Mot. at 14). The Government's arguments in support of those requests are reflected in its May 9, 2022 sealed, *ex parte* filing pursuant to CIPA § 6.